

# On the Power of Security Reduction in the Quantum-accessible Random Oracle Model

Jeeun Lee\*

Kwangjo Kim\*

**Abstract:** The advent of quantum computers and their algorithms has opened the era of post-quantum cryptography. Accordingly, new security proof models and proof techniques in a quantum setting need to be settled. As the classical random oracle (CRO) model is widely accepted as an efficient security proof tool, quantum-accessible random oracle (QaRO) model has been suggested by allowing the adversary's access to quantum computation. In this paper, we examine the features of CRO model and how they are applied to the QaRO model. Compared to the classical case, QaRO model has advantages such as quantum parallelism, but also weaknesses due to no-cloning theorem and collapse during measurement, e.g. adaptive programmability, rewinding, extractability, challenge injection, and oracle simulation. We review and compare the attempts to extend classical features to quantum one and how they overcome weaknesses, by introducing new quantum proof techniques.

**Keywords:** security reduction · quantum-accessible random oracle · adaptive programmability · rewinding · extractability · challenge injection · oracle simulation

## 1 Introduction

### 1.1 Motivation

As more and more refined classical, i.e. non-quantum, computers are developed, several problems have been encountered such as quantum tunnelling and heat generation. Quantum computers have been proposed as a natural solution to circumventing the aforementioned problems since 1970s. Quantum computers are based on quantum mechanics and use qubits to create quantum logic gates for quantum computing. Also, quantum computers use logically reversible manipulation of information where the output of a device always uniquely determines its input, by using an injective function for mapping old states to new ones. Such manipulation requires no release of heat in principle. For these reasons, quantum computing has attracted research interest both academically and commercially since its initial proposal.

After the publication of Deutsch's groundbreaking paper [Deu85], many quantum algorithms have been introduced such as Simon's algorithm [Sim94], Shor's algorithm [Sho94], and Grover's algorithm [Gro96]. When large-scale quantum computers are available, Shor's algorithm could break classical asymmetric encryption and digital signature schemes based on integer factorization and discrete logarithm problems in polynomial time. Also, classical symmetric encryption schemes would not be safe due to Grover's algorithm and Simon's algorithm.

In this manner, quantum security of the current classical cryptosystems has been investigated, and the cryptographic community has developed new security proof

models and proof techniques accordingly [BDF<sup>+</sup>11, BJ15, GHS16, Gag17, SLL16]. In this paper, we focus on the power of security reduction quantum-accessible random oracle (QaRO) model, compared to the classical random oracle (CRO) model, as it is accepted as an efficient and feasible proof model for provable security.

### 1.2 Organization

The rest of this paper is organized as follows: First, the extension of the random oracle model from a classical to quantum setting is explained and suitable security notions for QaRO model are discussed in Section 2. From Sections 3 to 7, we review useful features of the CRO model and how they are applied to the QaRO model; quantum adversaries are powerful by quantum parallelism but also have difficulties to extend classical features such as adaptive programmability, rewinding, extractability, challenge injection, and oracle simulation. Finally, we conclude by summarizing new quantum proof techniques and providing future work in Section 8.

## 2 Preliminaries

### 2.1 Quantum-accessible Random Oracle Model

A classical query algorithm that computes a Boolean function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  by using oracle queries is called a *decision tree*. A decision tree can be represented as a binary tree where each node represents a query, and its two children represent the two possible outcomes of the query. A leaf node represents the final answer 0 or 1. The depth of the tree, i.e. the number of queries needed to compute  $f$ , is the cost of an algorithm. This query model is useful in security proof since the number

\* School of Computing, KAIST, Daejeon 34141, South Korea.  
{jeeun.lee,kkj}@kaist.ac.kr

of queries, that an adversary needs to break a scheme, corresponds to the time the attack succeeds.

According to [BBC<sup>+</sup>98], a quantum query algorithm with  $q$  queries is a quantum analogue of a classical decision tree with  $q$  queries, where we use the power of quantum parallelism by making queries and operations in superposition. This can be represented as a sequence of unitary transformations:  $\hat{U}_q \hat{O}_f \cdots \hat{U}_1 \hat{O}_f \hat{U}_0$ . Here,  $\hat{U}_j$ 's are fixed unitary transformations that do not depend on inputs, and the (possibly) identical  $\hat{O}_f$ 's are unitary transformations that correspond to an oracle.

Consider a quantum system consisting of  $m$  qubits, with each qubit having basis states  $|0\rangle$  and  $|1\rangle$ , so that there are  $2^m$  possible basis states. Then the oracle transformation  $\hat{O}_f$ , called *QaRO*, maps basis state  $|x, y, z\rangle$  to  $|x, y \oplus f(x), z\rangle$ , where the length of query register,  $x$ , is  $\lceil \log n \rceil$  qubits, the length of answer register,  $y$ , is one qubit, the length of ancilla register,  $z$ , is an arbitrary string of  $m - \lceil \log n \rceil - 1$  qubits, and  $\oplus$  is exclusive or. Besides the *standard* transformation which maps basis state  $|x, y\rangle$  to  $|x, y \oplus g(x)\rangle$  for a general function  $g : \{0, 1\}^n \rightarrow \{0, 1\}^m$ , there can be different transformations to implement an oracle such as *Fourier phase* oracle  $|x, y\rangle \rightarrow e^{2\pi i g(x)y/2^m} |x, y\rangle$  and *minimal* oracle  $|x\rangle \rightarrow |g(x)\rangle$ . Using the standard oracle, the following quantum encryption oracle is used for constructing post-quantum security notions in Section 2.2:  $\hat{O}_{\text{Enc}_k}$  mapping basis state  $|m, c\rangle$  to  $|m, c \oplus \text{Enc}_k(m)\rangle$ .

After the quantum query algorithm is applied to an oracle-independent initial state, we can get an oracle-dependent final state. Finally, the computation ends with some measurement or observation of the final state.

## 2.2 Post-quantum Security Notions

The security notions are defined by pairing of a particular goal and a particular attack model. As one of possible security goals, *indistinguishability* formalizes an adversary's advantage to distinguish the encryptions of two plaintexts of the same length. As possible attack models, three different attacks are considered: *chosen-plaintext attack* (CPA), *non-adaptive chosen-ciphertext attack* (CCA1), and *adaptive chosen-ciphertext attack* (CCA2). Under CPA, the adversary has an encryption oracle access and obtains ciphertexts for plaintexts of their choice. Under CCA1, the adversary has an additional decryption oracle access before the challenge phase, whereas under CCA2, the adversary has an additional decryption oracle access before and after the challenge phase. The CCA2 adversary, however, is not allowed to query the challenge ciphertext itself to the decryption oracle. Hence, the decryption oracle after the challenge phase is modified as follows:

$$\text{Dec}_k^{c_b}(c) = \begin{cases} \perp & \text{if } c = c_b, \\ \text{Dec}_k(c) & \text{otherwise.} \end{cases}$$

In the QaRO model, we consider the adversary having an access to the quantum encryption oracle provided by an external challenger, instead of having a direct

access to the quantum encryption oracle, to rule out far too powerful adversaries. Then the following security notions are reasonable and achievable in this QaRO model: *indistinguishability under quantum ATK* (IND-qATK) [BZ13], *weak-quantum indistinguishability under quantum ATK* (wqIND-qATK), and *quantum indistinguishability under quantum ATK* (qIND-qATK) [GHS16, Gag17]. It should be noted that IND-qATK game uses standard transformation  $\hat{O}_{\text{Enc}_k}$ , where  $(\hat{O}_{\text{Enc}_k})^\dagger \neq \hat{O}_{\text{Dec}_k}$ , whereas (wqIND/qIND)-qATK game uses minimal transformation  $\hat{O}'_{\text{Enc}_k}$ , where  $(\hat{O}'_{\text{Enc}_k})^\dagger = \hat{O}'_{\text{Dec}_k}$  for quantum encryption oracles. Therefore, for devices using standard transformation, it would be sufficient to be IND-qATK secure.

**Definition 2.1 (IND-qATK for  $\Pi_{\text{sym}}$ ).** For  $\text{ATK} \in \{\text{CPA}, \text{CCA1}, \text{CCA2}\}$ , a symmetric encryption scheme  $\Pi_{\text{sym}}$  is said to be IND-qATK secure if the advantage of any quantum probabilistic polynomial-time adversary  $\mathcal{A} = (\mathcal{A}_M, \mathcal{A}_D)$ , where  $\mathcal{A}_M$  and  $\mathcal{A}_D$  are a message generator and a distinguisher, respectively, winning the game is negligible.

$$\text{Adv}_{\mathcal{A}, \Pi_{\text{sym}}}^{\text{IND-qATK}}(\lambda) := 2 \cdot \text{Succ}_{\mathcal{A}, \Pi_{\text{sym}}}^{\text{IND-qATK}} - 1 = \text{negl}(\lambda),$$

where  $\text{Succ}_{\mathcal{A}, \Pi_{\text{sym}}}^{\text{IND-qATK}}$  is as follows:

$$\Pr \left[ \begin{array}{l} k \xleftarrow{\$} \text{KeyGen}(1^\lambda); (m_0, m_1, |\text{state}\rangle) \xleftarrow{\$} \mathcal{A}_M^{O_1}; \\ b \xleftarrow{\$} \{0, 1\}; c_b \xleftarrow{\$} \mathcal{O}_{\text{Enc}_k}(m_b); \\ b' \leftarrow \mathcal{A}_D^{O_2}(c_b, |\text{state}\rangle) : b' = b \end{array} \right] \text{ for}$$

$$(\text{ATK}, \mathcal{O}_1, \mathcal{O}_2) = \begin{cases} (\text{CPA}, \hat{O}_{\text{Enc}_k}, \hat{O}_{\text{Enc}_k}) \\ (\text{CCA1}, \{\hat{O}_{\text{Enc}_k}, \hat{O}_{\text{Dec}_k}\}, \hat{O}_{\text{Enc}_k}) \\ (\text{CCA2}, \{\hat{O}_{\text{Enc}_k}, \hat{O}_{\text{Dec}_k}\}, \{\hat{O}_{\text{Enc}_k}, \hat{O}_{\text{Dec}_k}^{c_b}\}). \end{cases}$$

## 3 Adaptive Programmability of QaRO

Following [Nie02, FLR<sup>+</sup>10, BM15], as an important feature of the CRO model, *programmability* allows security reductions to dynamically select the outputs of an ideal hash function. For a standard security reduction technique, where the reduction tries to break the underlying hardness assumption, the reduction having oracle access to the adversary simulates the random oracle by answering queries made by the adversary. A random oracle can be simulated by adaptively setting or programming the outputs to a value of reduction's choice. As long as the distribution of the programmed output is uniform on the specified range, any method for selecting these values is permitted.

If a reduction in the CRO model is *history-free*, then it can also be carried out in the QaRO model as in Theorem 3.1. History-free reductions basically answer random oracle queries independently of the history of previous queries. Since many signature schemes have security reductions involving reprogramming in the CRO model, i.e. not history-free, security reductions in the

QaRO model is not known to hold. For reductions that are not history-free, adaptive reprogramming of the QaRO is required.

**Theorem 3.1** ([BDF<sup>+</sup>11, Theorem 1]). *Let  $\mathcal{S} = (G, S, V)$  be a signature scheme. Suppose that there is a history-free reduction that uses a classical PPT adversary  $A$  for  $\mathcal{S}$  to construct a PPT algorithm  $B$  for a problem  $P$ . Further, assume that  $P$  is hard for polynomial-time quantum computers, and that quantum-accessible pseudorandom functions exist. Then  $\mathcal{S}$  is secure in the QaRO model.*

The CRO model allows adaptive programming, i.e. the reduction can program the random oracle adaptively in the online phase of the security game depending on the query received from the adversary. In the QaRO model, however, it was considered to be difficult to program the random oracle adaptively since the quantum adversary can query the random oracle with a superposed state and get information about all exponentially many values right at the beginning.

### 3.1 Using One-way to Hiding Lemma

In order to program adaptively in the QaRO model, new techniques were developed by [Unr14] for the first time. It allows us to reduce the probability that the adversary notices that a random oracle has been reprogrammed to the probability of said adversary querying the oracle at the programmed location. It might be relatively trivial in the CRO model, but becomes non-trivial when the adversary can query superposed states:

**Theorem 3.2 (Adaptive Programming of QaRO [Unr14, Theorem 10]).** *Let  $H : M \rightarrow N$  be a random oracle for finite  $M, N$ . (Infinite  $M \subseteq \{0, 1\}^*$  is also permissible.) Consider the following algorithms:*

- The oracle algorithm  $A_0$  that makes at most  $q_0$  queries to  $H$ .
- The classical algorithm  $A_C$  that may access the classical part of the final state of  $A_0$ . Assume that for every initial state, the output of  $A_C$  has collision entropy at least  $k$ .
- The oracle algorithm  $A_1$  that may access the final states of  $A_0$  and  $A_C$ .
- The oracle algorithm  $A_2$  that may access the final state of  $A_1$ ; and  $A_1$  and  $A_2$  together perform at most  $q_{12}$  queries to  $H$ .
- Let  $C_1$  be an oracle algorithm that on input  $(j, B, x)$  does the following: run  $A_1^H(x, B)$  until (just before) the  $j$ -th query, measure the argument of the query in the computational basis, output the measurement outcome. (When  $A_1$  makes less than  $j$  queries,  $C_1$  outputs  $\perp \notin \{0, 1\}^l$ .)

Let

$$P_A^1 := \Pr \left[ b' = 1 : H \stackrel{\$}{\leftarrow} (M \rightarrow N), A_0^H(), x \leftarrow A_C(), \right. \\ \left. A_1^H(x, H(x)), b' \leftarrow A_2^H(x, H(x)) \right]$$

$$P_A^2 := \Pr \left[ b' = 1 : H \stackrel{\$}{\leftarrow} (M \rightarrow N), A_0^H(), x \leftarrow A_C(), \right. \\ \left. B \stackrel{\$}{\leftarrow} N, A_1^H(x, B), H(x) := B, b' \leftarrow A_2^H(x, B) \right]$$

$$P_C := \Pr \left[ x = x' : H \stackrel{\$}{\leftarrow} (M \rightarrow N), A_0^H(), x \leftarrow A_C(), \right. \\ \left. B \stackrel{\$}{\leftarrow} N, j \stackrel{\$}{\leftarrow} \{1, \dots, q_{12}\}, x' \leftarrow C_1^H(j, B, x) \right]$$

$$\text{Then } |P_A^1 - P_A^2| \leq (4 + \sqrt{2})\sqrt{q_0}2^{-k/4} + 2q_{12}\sqrt{P_C}.$$

### 3.2 Using Hardness of Witness-Search Game

In Theorem 3.2, the oracle is queried at an adversarially chosen  $x$  which is *information-theoretically* undetermined, possessing a high min-entropy,  $\min_x(-\log \Pr[X = x])$ . By extending it to a computational setting, [ES15] came up with a new technique when the input is *computationally* difficult to decide by the adversary. They formalized a probabilistic game called *witness-search* and showed the computational hardness of witness-search allows for adaptively programming a QaRO.

Let  $\text{Samp}$  be an instance-sampling algorithm. On input  $1^n$ ,  $\text{Samp}$  generates public information  $pk$ , description of a predicate  $P$ , and a witness  $w$  satisfying  $P(pk, w) = 1$ . The witness-search game  $\text{WS}$  is defined as below:

**Definition 3.1 (Witness-Search Game [ES15]).**

- Challenger  $\mathcal{C}$  generates  $(pk, w, P) \leftarrow \text{Samp}(1^n)$ . Ignore  $w$ . Let  $W_{pk} := \{w : P(pk, w) = 1\}$  be the collection of valid witnesses.
- $\mathcal{A}$  receives  $pk$  and produces a string  $\hat{w}$  as output.
- We say  $\mathcal{A}$  wins the game if  $\hat{w} \in W_{pk}$ .

**Lemma 3.1 (Hardness of WS to Programming QaRO [ES15, Lemma 5]).** *Let two experiments  $E$  and  $E'$  be as below. If  $\text{WS}$  is hard, then  $\text{Adv} := |\Pr_E[b = 1] - \Pr_{E'}[b = 1]| \leq \text{negl}(n)$ .*

- Experiment  $E$ :
  - Generate  $(pk, w, P) \leftarrow \text{Samp}(1^n)$ .
  - $\mathcal{O} \leftarrow \mathcal{F}$  is drawn uniformly at random from the collection of all functions  $\mathcal{F}$ .
  - $\mathcal{A}_1$  receives  $pk$  as input and makes at most  $q_1$  queries to  $\mathcal{O}$ .  $\mathcal{A}_1$  produces a classical string  $x$ .
  - Set  $z := \mathcal{O}(x||w)$ .
  - $\mathcal{A}_2$  gets  $(x, w, z)$  and may access the final state of  $\mathcal{A}_1$ .  $\mathcal{A}_2$  makes at most  $q_2$  queries to  $\mathcal{O}$ . It outputs  $b \in \{0, 1\}$  at the end.
- Experiment  $E'$ :
  - Generate  $(pk, w, P) \leftarrow \text{Samp}(1^n)$ .
  - $\mathcal{O} \leftarrow \mathcal{F}$  is drawn uniformly at random from the collection of all functions  $\mathcal{F}$ .
  - $\mathcal{A}_1$  makes at most  $q_1$  queries to  $\mathcal{O}$ .  $\mathcal{A}_1$  produces a classical string  $x$ .

- Pick a random  $z \in_R \text{Range}(\mathcal{O})$ . Reprogram  $\mathcal{O}$  to  $\mathcal{O}'$ :  $\mathcal{O}'(y) = \mathcal{O}(y)$  except that  $\mathcal{O}'(x||w) = z$ .
- $\mathcal{A}_2$  gets  $(x, w, z)$  and may access the final state of  $\mathcal{A}_1$ .  $\mathcal{A}_2$  makes at most  $q_2$  queries to  $\mathcal{O}'$ . It outputs  $b \in \{0, 1\}$  at the end.

Lemma 3.1 shows the computational assumption implies indistinguishability of two functions which a distinguisher has quantum access to: one is the zero function and the other marks a set of strings that could be used to break the computational assumption. Since the two functions are indistinguishable, any efficient quantum algorithm querying the random oracle cannot notice whether they have reprogrammed the QaRO.

### 3.3 Adaptive Reprogramming in TESLA

[ABB<sup>+</sup>17] gave a concrete tight security reduction for a signature scheme called TESLA, a lattice-based digital signature scheme, in the QaRO model. Their security reduction from learning with errors assumption adaptively reprograms QaRO using a technique from [BBBV97].

## 4 Rewinding of QaRO

The CRO model uses *rewinding* [PS96] as a powerful tool to construct an extractor which extracts the witness  $w$  from the prover. Rewinding is a proof technique where the state of the adversary is stored and reproduced later, that is, it should be possible to make snapshots of the state and then later to go back to that snapshot.

In the QaRO model, however, it is difficult to rewind by reversing the unitary transformation or taking snapshots in a quantum setting due to no-cloning theorem and collapse during measurement: snapshots cannot be copied and interacting with a simulated machine may destroy information that would be needed later [vdG97, Proposition 4.5].

### 4.1 Watrous' Rewinding

In order to resolve this issue, [Wat09] introduced a specific type of quantum rewinding: whenever some machine rewinds another machine to an earlier point, the rewinding machine forgets everything it learned after that point. [Wat09, Lemma 9] was reformulated as below:

**Lemma 4.1 (Quantum Rewinding with Small Perturbations [Unr10, Corollary 17]).** *Let  $C, Z, E, Y$  be quantum registers, where  $C$  is one qubit register. Let  $S_1$  be a unitary transformation operating on  $C, Z, Y$  and let  $\mathbf{M}$  be a measurement in the computational basis on register  $C$ .*

*For a quantum state  $|\Psi\rangle$ , let  $p(|\Psi\rangle) := \Pr[\text{Succ} = 1 : S_1(CZY), \text{Succ} \leftarrow \mathbf{M}(C)]$  where  $Z, E$  are jointly initialized with  $|\Psi\rangle$  and  $Y, C$  are initialized with  $|0\rangle$ . In the same situation, let the density operator  $\rho_{\Psi}^1$  denote the state of  $ZE$  in the case of  $\text{Succ} = 1$ .*

*Let  $\varepsilon \in (0, 1/2)$ . Let  $q \in (\varepsilon, 1/2]$ . Assume that for all  $|\Psi\rangle$ ,  $|p(|\Psi\rangle) - q| \leq \varepsilon$ .*

*Then there exists a quantum circuit  $S$  operating on  $Z$  of size  $O\left(\frac{\log(1/\varepsilon)\text{size}(S_1)}{(q-\varepsilon)(1-q+\varepsilon)} =: k\right)$ .  $S$  is a general quantum circuit, which may create auxiliary qubits, destroy them, and perform measurements.  $S$  can be computed in time  $O(k)$  given the description of  $S_1$ . And for any  $|\Psi\rangle$ ,*

$$\text{TD}(\rho_{\Psi}^1, \rho_{\Psi}^2) \leq 4\sqrt{\varepsilon} \frac{k}{\text{size}(S_1)},$$

*where the density operator  $\rho_{\Psi}^2$  denotes the state of  $ZE$  after execution of  $S$  when  $ZE$  is initialized with  $|\Psi\rangle$ .*

### 4.2 Unruh's Rewinding

A rewinding technique in the context of a specific two-prover commitment scheme was developed in [CSST11, Lemma 1], which was reformulated as below:

**Lemma 4.2 (Rewinding of mBQKW Commitment [Unr10, Lemma 10]).** *Consider two projectors  $P_0$  and  $P_1$  of the form  $P_i = U_i^\dagger(|\hat{w}_i\rangle\langle\hat{w}_i| \otimes I)U_i$ . (Here  $U_0, U_1$  are unitaries and  $\hat{w}_0, \hat{w}_1 \in \{0, 1\}^n$  for some  $n$ .) Consider a state  $|\psi\rangle$ . Let  $p_i := \|P_i|\psi\rangle\|^2$ . (That is,  $p_i$  is the probability of measuring  $\hat{w}_i$  in the first register after applying  $U_i$  to  $|\psi\rangle$ .) Let  $p_{\oplus} := \|P_1P_0|\psi\rangle\|^2$ . (That is,  $p_{\oplus}$  is the probability of measuring  $\hat{w}_0$  after applying  $U_0$  to  $|\psi\rangle$  and subsequently measuring  $\hat{w}_1$  after applying  $U_1U_0^\dagger$ .)*

*Assume that  $p_0 + p_1 \geq 1 + \varepsilon$  for some  $\varepsilon \geq 0$ . Then  $p_{\oplus} \geq \varepsilon^2/4$ .*

[Unr10] pointed out that Lemma 4.1 technique only can be used to backtrack if the rewinding machine made a mistake that should be corrected, but cannot be used to collect and combine information from different branches of an execution. Also, Lemma 4.2 is specific to the case where there are only two possible measurements, i.e.  $\#C = 2$ . [Unr10] developed a new rewinding technique, by showing that the output that is measured contains little information about the state and thus does not disturb the state too much, of which core lemma is as below:

**Lemma 4.3 (Extraction via Quantum Rewinding [Unr10, Lemma 8]).** *Let  $C$  be a set with  $\#C = c$ . Let  $(P_i)_{i \in C}$  be orthogonal projectors on a Hilbert space  $\mathcal{H}$ . Let  $|\Phi\rangle \in \mathcal{H}$  be a unit vector. Let  $V := \sum_{i \in C} \frac{1}{c} \|P_i|\Phi\rangle\|^2$  and  $E := \sum_{i, j \in C, i \neq j} \frac{1}{c^2} \|P_iP_j|\Phi\rangle\|^2$ . Then, if  $V \geq \frac{1}{\sqrt{c}}$ ,  $E \geq V(V^2 - \frac{1}{c})$ .*

It should be noted that strict soundness is additionally required while only special soundness is needed in a classical setting.

**Definition 4.1 (Special Soundness [Unr10, Definition 5]).** *We say a  $\Sigma$ -protocol  $(P, V)$  for a relation  $R$  has special soundness if there is a deterministic polynomial-time algorithm  $K_0$  (the special extractor) such that the following holds: for any two accepting conversations  $(\text{com}, \text{ch}, \text{resp})$  and  $(\text{com}, \text{ch}', \text{resp}')$  for  $x$  such that  $\text{ch} \neq \text{ch}'$  and  $\text{ch}, \text{ch}' \in C_x$ , we have that  $w := K_0(x, \text{com}, \text{ch}, \text{resp}, \text{ch}', \text{resp}')$  satisfies  $(x, w) \in R$ .*

**Definition 4.2 (Strict Soundness [Unr10, Definition 6]).** We say a  $\Sigma$ -protocol  $(P, V)$  has strict soundness if for any two accepting conversations  $(\text{com}, \text{ch}, \text{resp})$  and  $(\text{com}, \text{ch}, \text{resp}')$  for  $x$ , we have that  $\text{resp} = \text{resp}'$ .

## 5 Extractability of QaRO

The *extractability* or *pre-image awareness*, i.e. the simulator learns the pre-images the adversary is interested in, is crucial to simulate decryption queries in the security proof for OAEP in the CRO model [Fis05]. In the QaRO model, it is unclear how to extract the right query since the actual query may be hidden in a superposition of exponentially many states. The different definition is needed in a quantum setting; we do not give the extractor the power to see the oracle queries.

### 5.1 Unruh’s extractability

The *online extractability* was defined for an extractor, an algorithm  $E(H, x, \pi)$  where  $H$  is assumed to be a description of the random oracle,  $x$  a statement and  $\pi$  a proof of  $x$  as below.  $E$  is supposed to output a witness. Inputs and outputs of  $E$  are classical.

**Definition 5.1 (Online Extractability [Unr14, Definition 3]).** A non-interactive proof system  $(P, V)$  is online extractable with respect to  $S_{\text{init}}$  iff there is a polynomial-time extractor  $E$  such that for any quantum-polynomial-time oracle algorithm  $A$ , we have that

$$\Pr[\text{ok} = 1 \wedge (x, w) \notin R : H \leftarrow S_{\text{init}}(), (x, \pi) \leftarrow A^H(), \\ \text{ok} \leftarrow V^H(x, \pi), w \leftarrow E(H, x, \pi)]$$

is negligible. We assume that both  $S_{\text{init}}$  and  $E$  have access to and may depend on a polynomial upper bound on the runtime of  $A$ .

The definition implies that it is impossible for an adversary to produce a proof for a statement for which he does not know a witness. The case, when the adversary can take one proof  $\pi_1$  for one statement  $x_1$  and transform  $\pi_1$  into a valid proof for another statement  $x_2$ , however, is not excluded as long as a witness for  $x_2$  could efficiently be computed from a witness for  $x_1$ . It is usually referred to as malleability. Therefore, simulation soundness, i.e. extraction of a witness from the adversary-generated proof should be successful even if the adversary has access to simulated proofs, is adapted to online extractability to avoid malleability:

**Definition 5.2 (Simulation-sound Online Extractability [Unr14, Definition 4]).** A non-interactive proof system  $(P, V)$  is simulation-sound online extractable with respect to  $(S_{\text{init}}, S_P)$  iff there is a polynomial-time extractor  $E$  such that for any quantum-polynomial-time oracle algorithm  $A$ , we have that

$$\Pr[\text{ok} = 1 \wedge (x, \pi) \notin \text{simproofs} \wedge (x, w) \notin R : \\ H \leftarrow S_{\text{init}}(), (x, \pi) \leftarrow A^{H, S_P}(), \\ \text{ok} \leftarrow V^H(x, \pi), w \leftarrow E(H, x, \pi)]$$

is negligible. Here *simproofs* is the set of all proofs returned by  $S_P$  (together with the corresponding statements).

We assume that both  $S_{\text{init}}, S_P$  and  $E$  have access to and may depend on a polynomial upper bound on the runtime of  $A$ .

The simulation-sound online extractability allows us to extract a witness from a successful adversary without measuring or rewinding, and avoids the problem of determining the query inputs by including its outputs in the proof and inverting them in the security proof. We do not need to operate in any way on the quantum state of the adversary and get the witness purely by inspecting the classical proof/signature. It avoids the usual problem of disturbing the quantum state while trying to extract a witness.

## 6 Challenge Injection of QaRO

In the CRO model, many reductions succeed by injecting a challenge into one of the responses to the random oracle; a random query was selected, and rather than responding in the usual way, the reduction algorithm responded with the element  $r$  that was provided by the challenger [Eat17]. In the QaRO model, a random query cannot be simply responded to by returning the classical element  $r$ .

### 6.1 Zhandry’s Technique

One possible solution is to choose a random subset  $D$  of the domain  $\mathcal{D}$  and define the oracle  $H$  so that for any  $d \in D$ ,  $H(d) = y$ , the challenge point. The question then is if it is possible to choose  $D$  in such a way that it is large enough so that we can reasonably hope for the forgery to be associated with  $y$ , but not so large that the adversary notices that our oracle isn’t a true random oracle. This was possible by defining a construction called *semi-constant distribution* as below:

**Definition 6.1 (Semi-constant Distribution [Zha12, Definition 4.1]).** The semi-constant distribution  $\text{SC}_{\lambda, y}$  is a distribution on mappings from a domain  $\mathcal{D}$  to a range  $\mathcal{R}$ . It is parameterized by a value  $\lambda \in [0, 1]$  and an element  $y \in \mathcal{R}$ . The distribution is defined by how it is sampled. For each  $d \in \mathcal{D}$ , with probability  $\lambda$  set  $H(d) = y$ . Otherwise set it to a uniformly random element of  $\mathcal{R}$ .

Then the following theorem was proved:

**Corollary 6.1 ([Zha12, Corollary 4.3]).** If  $y$  is a uniformly random element of  $\mathcal{R}$ , then the distribution of any quantum algorithm that makes  $q$  queries to a random oracle has distance at most  $\frac{8}{3}q^4\lambda^2$  from the distribution generated when  $\text{SC}_{\lambda, y}$  is used instead.

Using the above technique regarding indistinguishability of oracles against quantum adversaries, [Zha12] provided the security of [GPV08]’s identity-based encryption (GPV-IBE) scheme in the QaRO model. Though

Zhandry’s technique is general and useful, a huge reduction loss and a wide gap between the concrete efficiency and security level in the CRO and QaRO model are unavoidable because the reduction algorithm has to abort with high probability.

## 6.2 KYY’s Technique

Recently, [KYY18] provided a much tighter security proof for single-challenge GPV-IBE scheme in the QaRO model as in Theorem 6.1. Also, multi-challenge GPV-IBE scheme has an almost tight reduction in the QaRO model as in Theorem 6.2. KYY’s technique uses completely different approach from Zhandry’s by simulating in a way so that exactly one valid secret key for every identity can be created.

**Theorem 6.1 ([KYY18, Theorem 2]).** *The GPV-IBE scheme is adaptively-anonymous single-challenge secure assuming the hardness of  $\text{LWE}_{n,m,q,\chi}$  in the QaRO model, where  $\chi = D_{\mathbb{Z},\alpha q}$ . Namely, for any quantum adversary  $\mathcal{A}$  making at most  $Q_H$  queries to  $|H\rangle$  and  $Q_{ID}$  secret key queries, there exists a quantum algorithm  $\mathcal{B}$  making  $Q_H + Q_{ID}$  QaRO queries such that*

$$\text{Adv}_{\mathcal{A},\text{GPV}}^{\text{IBE}}(\lambda) \leq \text{Adv}_{\mathcal{B},\text{QaRO}_{l_r,l_r}}^{\text{LWE}_{n,m,q,\chi}}(\lambda) + (Q_H^2 + Q_{ID}) \cdot 2^{-\Omega(n)}$$

and

$$\text{Time}(\mathcal{B}) = \text{Time}(\mathcal{A}) + (Q_H + Q_{ID}) \cdot \text{poly}(\lambda),$$

where  $l_r$  denotes the length of the randomness for  $\text{Sample}\mathbb{Z}$ .

**Theorem 6.2 ([KYY18, Theorem 4]).** *The GPV-IBE scheme is adaptively-anonymous multi-challenge secure assuming the hardness of  $\text{LWE}_{l,m,q,\chi}$  in the QaRO model, where  $\chi = D_{\mathbb{Z},\alpha q}$ . Namely, for any quantum adversary  $\mathcal{A}$  making at most  $Q_H$  queries to  $|H\rangle$ ,  $Q_{ch}$  challenge queries, and  $Q_{ID}$  secret key queries, there exists a quantum algorithm  $\mathcal{B}$  making at most  $3Q_H + 6Q_{ch} + 2Q_{ID}$  QaRO queries such that*

$$\text{Adv}_{\mathcal{A},\text{GPV}_{\text{mult}}}^{\text{IBE}}(\lambda) \leq 3n \cdot \text{Adv}_{\mathcal{B},\text{QaRO}_{l_r+2,\max\{l_r,(\lceil \log q \rceil + 2\lambda) \times n\}}}^{\text{LWE}_{l,m,q,\chi}}(\lambda) + (Q_H + Q_{ch} + Q_{ID}) \cdot 2^{-\Omega(n)}$$

and

$$\text{Time}(\mathcal{B}) = \text{Time}(\mathcal{A}) + (Q_H + Q_{ch} + Q_{ID}) \cdot \text{poly}(\lambda),$$

where  $l_r$  denotes the length of the randomness for  $\text{Sample}\mathbb{Z}$ .

## 7 Efficient Simulation of QaRO

In the CRO model, simulating an exponential-size random oracle is efficient via *lazy sampling*. As queries to the random oracle are received, a table is built up of queries and responses. When a query is submitted that isn’t in the table, a random output is generated as a response, and the query and the output are recorded in the table. By doing this, the simulation is entirely indistinguishable from a truly random oracle, and the reduction algorithm only needs to maintain a table with

size at most  $q$  [Eat17]. However, in the CRO model, managing such a table is infeasible because the adversary can submit a superposition of all inputs as his first query, which requires the oracle to be defined for all possible inputs when the first query is made.

The *quantum-accessible pseudorandom functions* are proposed as a solution in [BDF<sup>+</sup>11], where the distinguisher is given quantum access to  $O$  or  $f$  by way of the unitary mapping  $U_O$  or  $U_f$ . Although they are an efficient and flexible replacement for a QaRO, an additional computational assumption should be introduced whereas the CRO model does not need such assumption as queries can be answered as they are made in a uniform and independent way.

As another solution, [Zha12] proposed  $k$ -wise independent functions to simulate the QaRO.

**Definition 7.1 ([Zha12]).** *A family of  $k$ -wise independent functions is a set  $\mathcal{F}$  of functions  $f : \mathcal{D} \rightarrow \mathcal{R}$  such that if  $d_1, \dots, d_k$  are any  $k$  different elements of  $\mathcal{D}$  and  $r_1, \dots, r_k$  are any  $k$  elements of  $\mathcal{R}$  (possible with repeats), then*

$$\Pr_{f \leftarrow \mathcal{F}} [f(d_1) = r_1 \wedge f(d_2) = r_2 \wedge \dots \wedge f(d_k) = r_k] = \frac{1}{|\mathcal{R}|^k}.$$

Intuitively, a  $k$ -wise independent function is a function that appears perfectly uniform and independent if you look at no more than  $k$  input/output pairs. The following theorem establishes how these functions may be used to replace the QaRO.

**Theorem 7.1 ([Zha12]).** *Let  $\mathcal{A}$  be a quantum algorithm outputting some classical state  $z$ , that makes  $q$  quantum queries to a random oracle  $\mathcal{O} : \mathcal{D} \rightarrow \mathcal{R}$ , drawn uniformly from the set of all such functions. If  $\mathcal{F}$  is a family of  $2q$ -wise independent functions  $f : \mathcal{D} \rightarrow \mathcal{R}$ , then*

$$\Pr[\mathcal{A}^{\mathcal{O}} \rightarrow z] = \Pr_{f \leftarrow \mathcal{F}} [\mathcal{A}^f \rightarrow z].$$

## 8 Summary of Quantum Techniques

Since quantum computers have been suggested as a solution of classical computers and attracted interest both academically and commercially, cryptographic community is needed to consider the threats of quantum computers to current classical cryptosystems. As CRO model has been regarded as an efficient security proof tool, [BDF<sup>+</sup>11] introduced QaRO model to prove quantum security of classical cryptosystems. The QaRO model allows quantum adversaries’ access to quantum computation such as superposition of inputs to random oracle, which gives quantum advantages, however, there are some weaknesses that cannot be extended naturally from classical RO model. We investigated the difficulties of security reduction in the QaRO model, which caused by quantum mechanical properties such as no-cloning theorem and collapse during measurement: adaptive programmability, rewinding, extractability, challenge injection, and efficient simulation of QaRO.

It was shown that if a reduction in the CRO model is history-free, then it can also be applied in the QaRO model. Many classical schemes are not history-free, i.e. of which security reductions involves reprogramming in the CRO model, adaptive reprogramming in the QaRO model is also required to prove such schemes. As a first attempt, the adaptive programming of QaRO based on one-way to hiding lemma and the computational hardness of witness-search game was developed. Recently, the security reduction of lattice-based digital signature scheme called TESLA was given in a quantum setting by adaptively reprogramming QaRO.

Also, it was considered to be difficult to rewind QaRO as CRO since the adversary cannot store and reproduce the state. [Wat09] and [Unr10] introduced quantum version of rewinding, even though it only can be applied to a specific case: Watrous' rewinding cannot be used to collect and combine information from different branches of an execution, and Unruh's rewinding requires strict soundness that does not needed in the CRO model.

The extractability of QaRO is not easily extended from CRO model because the actual query may be hidden in a superposed state, so different definition was suggested by not giving the extractor the power to see the oracle queries. [Unr14] defined an online extractability and simulation-sound online extractability to allow us to extract a witness from a successful adversary without measuring or rewinding. It operates in non-invasive way and avoids disturbing quantum states while trying to extract a witness.

There are other difficulties such as challenge injection and oracle simulation. The difficulties of challenge injection in the QaRO model was resolved by defining semi-constant distribution and giving the theorem for enabling challenge injection [Zha12]. The recent work [KYY18] pointed out a huge reduction loss of Zhandry's technique and provided tighter security reduction of GPV-IBE scheme in the QaRO model. Zhandry also proposed  $k$ -wise independent functions to simulate the QaRO, instead of using quantum-accessible pseudorandom functions to avoid using additional computational assumption. The Corollary 6.1 from  $k$ -wise independent functions showed these functions can replace to QaRO.

## 9 Future Work

Due to quantum mechanical properties, the security reduction by quantum adversaries have both strengths and weaknesses during security proofs. We investigated known weaknesses in this paper, but there might be more difficulties to concretely define QaRO by extending CRO model. We will study new properties of quantum adversaries in detail, and if there are limitations in quantum security proof, give new quantum proof techniques to overcome problems.

## Acknowledgements

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korean government (MSIT) (No. 2017-0-00555, Towards provable-secure multi-party authenticated key exchange protocol based on lattices in a quantum world).

## References

- [ABB<sup>+</sup>17] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, and F. Pawlega. Revisiting TESLA in the quantum random oracle model. In *Proceedings of the 8th International Workshop on Post-Quantum Cryptography (PQCrypto 2017)*, pages 143–162, Utrecht, The Netherlands, June 2017.
- [BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.
- [BBC<sup>+</sup>98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS 1998)*, Palo Alto, CA, USA, November 1998.
- [BDF<sup>+</sup>11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *Proceedings of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2011)*, pages 41–69, Seoul, South Korea, December 2011.
- [BJ15] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity, June 2015. <https://arxiv.org/abs/1412.8766>.
- [BM15] R. Bhattacharyya and P. Mukherjee. Non-adaptive programmability of random oracle. *Theoretical Computer Science*, 592:97–114, August 2015.
- [BZ13] D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. Cryptology ePrint Archive, Report 2013/088, 2013. <https://eprint.iacr.org/2013/088>.
- [CSST11] C. Crépeau, L. Salvail, J.-R. Simard, and A. Tapp. Two provers in isolation. In *Proceedings of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2011)*, pages 407–430, Seoul, South Korea, December 2011.
- [Deu85] D. E. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, July 1985.

- [Eat17] E. Eaton. Signature schemes in the quantum random-oracle model. Master’s thesis, University of Waterloo, April 2017.
- [ES15] E. Eaton and F. Song. Making existential-unforgeable signatures strongly unforgeable in the quantum random-oracle model. In *Proceedings of the 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015)*, pages 147–162, Brussels, Belgium, May 2015.
- [Fis05] M. Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In *Proceedings of the 25th Annual International Cryptology Conference (Crypto 2005)*, pages 152–168, Santa Barbara, CA, USA, August 2005.
- [FLR<sup>+</sup>10] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam, and S. Tessaro. Random oracles with(out) programmability. In *Proceedings of the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2010)*, pages 303–320, Singapore, December 2010.
- [Gag17] T. Gagliardoni. *Quantum security of cryptographic primitives*. PhD thesis, Technische Universität Darmstadt, February 2017.
- [GHS16] T. Gagliardoni, A. Hülsing, and C. Schaffner. Semantic security and indistinguishability in the quantum world. In *Proceedings of the 36th Annual International Cryptology Conference (Crypto 2016)*, pages 60–89, Santa Barbara, CA, USA, August 2016.
- [GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008)*, pages 197–206, New York, NY, USA, May 2008.
- [Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996)*, pages 212–219, Philadelphia, PA, USA, May 1996.
- [KYY18] S. Katsumata, S. Yamada, and T. Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In *Proceedings of the 24th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2018)*, pages 253–282, Brisbane, QLD, Australia, December 2018.
- [Nie02] J. B. Nielsen. Separating random oracle proofs from complexity theoretic proofs: the non-committing encryption case. In *Proceedings of the 22nd Annual International Cryptology Conference (Crypto 2002)*, pages 111–126, Santa Barbara, CA, USA, August 2002.
- [PS96] D. Pointcheval and J. Stern. Security proofs for signature schemes. In *Proceedings of the 15th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 1996)*, pages 387–398, Saragossa, Spain, May 1996.
- [Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 124–134, Santa Fe, NM, USA, November 1994.
- [Sim94] D. R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 116–123, Santa Fe, NM, USA, November 1994.
- [SLL16] T. Shang, Q. Lei, and J. Liu. Quantum random oracle model for quantum digital signature. *Physical Review A*, 94:042314, October 2016.
- [Unr10] D. Unruh. Quantum proofs of knowledge. Cryptology ePrint Archive, Report 2010/212, 2010. <https://eprint.iacr.org/2010/212>.
- [Unr14] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. Cryptology ePrint Archive, Report 2014/587, 2014. <https://eprint.iacr.org/2014/587>.
- [vdG97] J. van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Université de Montréal, December 1997.
- [Wat09] J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, May 2009.
- [Zha12] M. Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Proceedings of the 32nd Annual International Cryptology Conference (Crypto 2012)*, pages 758–775, Santa Barbara, CA, USA, August 2012.